INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 2 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

REGULATORY FRAMEWORK FOR COMBATTING CYBERSTALKING AND ONLINE HARASSMENT

AUTHORS – DHWANI VRAJESH VYAS* & RAJ ARVIND SHAH**, ASSISTANT PROFESSOR AT SEVA MANDAL EDUCATION SOCIETY'S SMT. KAMALABEN GAMBHIRCHAND SHAH LAW SCHOOL* & ASSISTANT PROFESSOR AT M.K.E.S COLLEGE OF LAW**

BEST CITATION - DHWANI VRAJESH VYAS & RAJ ARVIND SHAH, REGULATORY FRAMEWORK FOR COMBATTING CYBERSTALKING AND ONLINE HARASSMENT, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (2) OF 2025, PG. 74-76, APIS – 3920 – 0001 & ISSN - 2583-2344.

This article is published in the collaborated special issue of M.K.E.S. College of Law and the Institute of Legal Education (ILE), titled "Current Trends in Indian Legal Frameworks: A Special Edition" (ISBN: 978-81-968842-8-4).

ABSTRACT

The rapid proliferation of digital technologies has brought about unprecedented opportunities for communication and social interaction. However, this digital revolution has also ushered in a darker side, marked by the rise of cyberstalking and online harassment. These insidious behaviors, often facilitated by the anonymity and reach of the internet, can inflict severe emotional distress, reputational damage, and even physical harm on victims. This research article examines the evolving legal frameworks aimed at addressing cyberstalking and online harassment, exploring the challenges in defining and prosecuting these crimes, analyzing existing legislation across jurisdictions, and discussing the need for comprehensive and adaptive legal strategies to combat this growing menace. It also considers the role of technology companies and social media platforms in mitigating online abuse.

Keywords: Cybercrime, cyberstalking, online harassment, Information Technology Act, 2000

Introduction

In recent years, India has undergone a significant digital transformation characterized by notable advancements in technology and connectivity. Nevertheless, this evolution has also led to the emergence of a concerning phenomenon: the rapid increase in cybercrime. As India progresses towards a more interconnected and digitized society, cybercriminals are capitalizing on vulnerabilities, posing threats to individuals, businesses, and governmental institutions.[116]

Cybercrime is defined as illicit activities performed through digital platforms, often targeting computer systems, networks, and online environments. These criminal acts can take various forms, such as hacking, phishing, identity theft, financial fraud, ransomware attacks, and cyberstalking. The motivations behind cybercriminal behaviour are multifaceted, including the pursuit of financial rewards, espionage, personal grievances, and acts of terrorism. The proliferation of internet technology has led to the emergence of cybercriminals, who exploit the general public's limited understanding of technology and cyberspace. Consequently, cyberspace has

[116] https://scroll.in/article/1078478/indias-cyber-scam-epidemic-is-part-of-a-multibillion-global-industry-this-series-traces-a-full-arc

become inundated with these criminals, who perceive significant opportunities for financial gain.[117]

Cyberstalking and online harassment

Cyberstalking and online harassment represent significant challenges in today's digital environment. Unlike traditional forms of stalking and harassment, these behaviours leverage electronic communication technologies to inflict harm. The pervasive and relentless nature of online attacks, coupled with the potential for anonymity and rapid information dissemination, can greatly amplify the psychological impact on victims. Cyberstalking may manifest through unwanted and repeated emails or text messages, the public release of private information (doxing), threats of violence, and the use of tracking technologies.[118] Online harassment encompasses a broader spectrum of abusive behaviours, including hate speech, discriminatory remarks, personal insults, and the spread of damaging rumours.[119]

The legal framework addressing cyberstalking and online harassment is intricate and continually evolving. Jurisdictions around the globe are facing the challenge of modifying existing laws or creating new legislation to effectively respond to these emerging forms of abuse.

Legal Frameworks

The Information Technology Act, 2000 and the Indian Penal Code that can be used to address certain forms of cyberstalking and online harassment. However, there is a growing recognition of the need for more comprehensive legislation specifically targeting these offenses.

Information Technology Act, 2000

Section 66C – Identity Theft

Punishes fraudulent use of electronic signatures, passwords, or personal details.

Penalty: Imprisonment up to 3 years and fine up to ₹1 lakh.

Section 66D – Impersonation for Fraud

Covers cases where someone impersonates another person online to deceive or defraud.

Penalty: Imprisonment up to 3 years and fine up to ₹1 lakh.

Section 67 – Publishing Obscene Material

Criminalizes transmitting or publishing obscene material online.

Penalty: First conviction – Up to 3 years imprisonment + fine up to ₹5 lakh.

Subsequent conviction – Up to 5 years imprisonment + fine up to ₹10 lakh.

Section 67A, 67B – Sexual Content & Child Exploitation

Section 67A: Punishes publishing sexually explicit material.

Section 67B: Punishes child pornographic content.

The Bharatiya Nyaya Sanhita (BNS), which replaced the Indian Penal Code (IPC) on July 1, 2024, addresses cyberstalking and online harassment through several provisions:

Stalking (Section 78)

Following a woman and repeatedly contacting or attempting to contact her despite clear indications of disinterest.

Monitoring a woman's use of the internet, email, or any other form of electronic communication.

These provisions are designed to combat both physical and cyberstalking.

[117] YOGESH PRASAD KOLEKAR, THE ROLE OF INDIAN CYBERCRIME COORDINATION CENTRE IN SAFEGUARDING CYBERSPACE, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 4 (4) OF 2024, PG. 233-235, APIS – 3920 – 0001 & ISSN – 2583-2344.

[118] Kolekar, Y.P. (2015), Protection of Data under Information Technology Law in India, 27 April, 1-12. Available at SSRN:http://ssrn.com/abstract=2599493

[119] https://docs.manupatra.in/newsline/articles/Upload/FDF5EB3E-2BB1-44BB-8F1D-9CA06D965AA9.pdf

Sexual Harassment (Section 75): This section defines sexual harassment to include:

Physical contact and advances involving unwelcome and explicit sexual overtures.

A demand or request for sexual favors.

Showing pornography against the will of a woman.

Making sexually colored remarks.

These provisions encompass various forms of harassment, including those conducted online.

Voyeurism (Section 77)

Watching or capturing images of a woman engaging in a private act without her consent.

Disseminating such images.

This addresses issues related to the non-consensual recording and sharing of intimate images, a concern in online harassment cases.

Insulting the Modesty of a Woman (Section 79)

Uttering words, making sounds or gestures, or exhibiting objects intending to insult a woman's modesty.

Intruding upon the privacy of a woman.

These provisions can be applied to online actions that insult or violate a woman's privacy.

Legal Remedies for Victims of Cyberstalking & Online Harassment in India

Filing a Police Complaint

Victims can file an FIR at the nearest police station.

Cybercrime complaints can also be filed online via the National Cyber Crime Reporting Portal: https://cybercrime.gov.in

Women-Specific Helpline Services

1091 – Women's Helpline

181 – Women's Distress Helpline

Cyber Crime Cells

Most cities have dedicated Cyber Crime Cells where victims can file complaints.

Conclusion

Cyberstalking and online harassment pose significant risks to both individuals and society at large. The dynamic nature of online abuse necessitates ongoing adjustments to legal frameworks and technological measures. Although considerable advancements have been achieved in formulating legislation and increasing awareness regarding these matters, there is still a substantial amount of work to be accomplished. Legal approaches must effectively tackle the distinct challenges presented by the digital landscape, such as anonymity, jurisdictional issues, and the collection of evidence. Additionally, technology firms and social media platforms should assume a more proactive role in curbing and alleviating online abuse.[120]

Through collaborative efforts, governments, law enforcement, technology companies, and civil society organizations can foster a safer and more secure online environment for everyone. Further investigation is essential to understand the long-term effects of cyberstalking and online harassment on victims, assess the efficacy of various legal and technological responses, and establish best practices for preventing and addressing these detrimental behaviors.

[120] https://www.legalserviceindia.com/legal/article-1048-cyber-stalking-in-india.html